



## *What do I keep hearing about "phishing" and identity theft?*

Many people enjoy fishing. It can be relaxing and peaceful and if you are really lucky there may actually be fish involved. If you have ever actually gone fishing you might appreciate the old adage that there is a significant difference between "fishing" and "catching". Anyone can fish, but catching takes skill.

Fishing of a different sort has become a serious security threat. Dubbed "phishing", it involves luring unsuspecting computer users to take the cyber-bait much the same way fishermen lure a fish to take the worm.

Phishing scams can be described like this: **"Phishing attacks use "spoofed" e-mails and fraudulent websites with the attempt to trick unsuspecting Internet users into divulging confidential personal information** such as credit card numbers, account

usernames and passwords, social security numbers, etc.

By hijacking the trusted brands of well-known institutions, phishers are able to convince a small percentage of recipients to respond to their offers.

Phishing scams are a result of underlying security flaws in software or simply the result of poor judgment on the part of the user. However, there are things that you can do to keep from being victimized by these scams.



## 6 Steps To Protect Yourself from Phishing

While a lack of understanding is certainly a contributing factor to the success of phishing scams, it is difficult to keep up with the latest attack tools and techniques. We realize that you simply want to use your computer, not become a security guru. So, here are five steps you can take to keep from being victimized by the phishing scam du jour.

**1. Be Skeptical:** It is better to err on the side of caution. Unless you are 100% sure that a particular message is legitimate, assume it is not. **Never supply any personal or confidential information via email. This includes:**

- usernames
- passwords
- account numbers
- debit or credit card account numbers
- card expiration dates
- PIN numbers

You should not reply directly to the email in question.

**2. Use The Old-Fashioned Way:** An even safer means of verifying if an email regarding your account is legitimate or not is to simply pick up the phone. Rather than risking that you may somehow be emailing the attacker or misdirected to the attacker's replica web site, just call customer service and explain what the email stated. You can easily verify if there is truly a problem with your account or if this is simply a phishing scam.

**3. Do Your Homework:** When your bank statements or account details arrive, whether in print or through electronic means, analyze them closely. Make sure there are no transactions that you can't account for and that all of the decimals are in the right spots. If you find any problems contact the company or financial institution in question immediately to notify them.

**4. Use A Secure Website:** Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browser's address bar - it should be "https://" rather than just "http://".

**5. Report Suspicious Activity:** If you receive emails that are part of a phishing scam or even seem suspicious you should report them. Report suspicious emails to your ISP and be sure to also report them to the Federal Trade Commission (FTC) through [www.phishinginfo.org](http://www.phishinginfo.org)

**6. Be Safe:** Ensure that your browser is up to date and security patches applied. In particular, people who use the Microsoft Internet Explorer browser should immediately go to the Microsoft Security home page — <http://www.microsoft.com/security/> — to download a special patch relating to certain phishing schemes.

You can also visit [www.northernfcu.com](http://www.northernfcu.com) to see our Identity Theft Coach and find out how to protect yourself from ID Theft.



**Main Office**

120 Factory Street  
Watertown, New York 13601  
Phone: (315) 782-0155  
Fax: (315) 782-8684

**Branch Offices**

Commerce Branch  
1180 E. Commerce Drive  
Watertown, New York 13601  
Phone: (315) 785-5600  
Fax: (315) 785-6226

Adams Branch  
10924 US Route 11  
Adams, New York 13605  
Phone: (315) 232-2990  
Fax: (315) 232-3723

Gouverneur Branch  
145 East Main Street  
Gouverneur, New York 13642  
Phone: (315) 287-0356  
Fax: (315) 287-4074

Lowville Branch  
No. 4 Road, P.O. Box 147  
Lowville, New York 13367  
Phone: (315) 376-7303  
Fax: (315) 376-7326

[www.northernfcu.com](http://www.northernfcu.com)

# Watch Out For Phishing Scams!

